WHAT IS CLAIMED IS

1. A method for identification among at least first and second users communicating by means of a communication system, said method comprising the steps of:

providing a first unique identifier from said first user to said second user;

entering into an agreement between the various parties as to a first plurality of hash salts;

at said second user, performing a hash operation on one of (a) said first unique identifier and (b) a deterministic transformation of said first unique identifier, using the first salt from said plurality of salts, to thereby produce a first data hash (A);

at said second user, performing a hash operation on at least a portion of said first data hash (A) using the second of said plurality of hash salts (B), to thereby produce a second data hash (B);

at said second user, performing a hash operation on at least a portion of said first data hash (A) using the third of said plurality of hash salts (C), to thereby produce a third data hash (C);

at said second user, performing a hash operation on at least a portion of said third data hash (C) using the fourth of said plurality of hash salts (D), to thereby produce a fourth data hash (D);

at said second user, discarding said third data hash (C);

at said second user, performing a hash operation, using a further one of said plurality of hash salts (E), on at least a portion of one of (a) said first unique identifier and (b) data deterministically derived from said

unique identifier, to thereby produce a fifth data hash (E);

at said second user, generating a random number;

at said second user, encrypting said random number with a key which includes at least a deterministic transformation of said second data hash, to produce an encrypted random number, where said transformation is agreed to ahead of time;

at said first user, decrypting said encrypted random number using as a key using said at least a deterministic transformation of said second data hash, to extract said random number, to thereby form an extracted random number;

at said first user, transmitting to said second user both said extracted random number and said third data hash;

at said second user, performing a hash operation on said third data hash by the use of said fourth salt, to thereby generate a sixth data hash (F);

at said second user, comparing said fourth and sixth data hashes, and deeming said message to be from said first user; and

at said second user, discarding said third data hash.

2. A method according to claim 1, further comprising, after said steps, at said second user, of (a) performing a hash operation on one of (a) said first unique identifier and (b) a deterministic transformation of said first unique identifier, using the first salt from said plurality of salts, to thereby produce a first data hash (A) and (b) performing a hash operation, using a further one of

said plurality of hash salts (E), on at least a portion of one of (a) said first unique identifier and (b) data deterministically derived from said unique identifier, to thereby produce a fifth data hash (E), the step of:

discarding said first unique identifier.

3. A method for identification among at least first and second users communicating by means of a communication system, said method comprising the steps of:

providing a first unique identifier from said first user to said second user,

entering into an agreement between the various parties as to a first plurality of hash salts;

at said second user, performing a hash operation on one of (a) said first unique identifier and (b) a deterministic transformation of said first unique identifier, using the first salt from said plurality of salts, to thereby produce a first data hash (A);

at said second user, performing a hash operation on at least a portion of said first data hash (A) using the second of said plurality of hash salts (B), to thereby produce a second data hash (B);

at said second user, performing a hash operation on at least a portion of said first data hash (A) using the third of said plurality of hash salts (C), to thereby produce a third data hash (C);

at said second user, performing a hash operation on at least a portion of said third data hash (C) using the fourth of said plurality of hash salts (D), to thereby produce a fourth data hash (D);

at said second user, discarding said third data

hash (C);

at said second user, performing a hash operation, using a fifth one of said plurality of hash salts (E), on at least a portion of one of (a) said first unique identifier and (b) data deterministically derived from said unique identifier, to thereby produce a fifth data hash (E);

at said second user, storing said second and fourth data hashes in memory at locations established by said fifth data hash;

at said first user, performing a hash operation on at least a portion of one of (a) said first unique identifier and (b) data deterministically derived from said unique identifier, using said fifth data hash, to thereby produce a replica of said fifth data hash;

transmitting said replica of said fifth data hash from said first user to said second user;

at said second user, accessing said memory at locations established by said replica of said fifth data hash to obtain said second and fourth data hashes;

at said second user, generating a random number;

at said second user, encrypting said random number with a key which includes one of (a) said second data hash and (b) a deterministic transformation of said second data hash, to produce an encrypted random number, where said transformation is agreed to ahead of time;

at said first user, decrypting said encrypted random number using as a key using one of (a) said second data hash and (b) a deterministic transformation of said second data hash, to extract said random number, to thereby form an extracted random number;

transmitting from said first user to said second

user both said extracted random number and said third data hash;

at said second user, performing a hash operation on said third data hash by the use of said fourth salt, to thereby generate a sixth data hash (F);

at said second user, comparing said fourth and sixth data hashes, and deeming said message to be from said first user if they are identical; and

at said second user, discarding said third data hash.

4. A method according to claim 3, further comprising, after said step of, at said second user, storing said second and fourth data hashes in memory at locations established by said fifth data hash, the step of:

discarding said fifth data hash.